Privacy and Security Issues in Discovery and Litigation:

Boldly Going Where Disclosure Never Went Before

Cyberspace Committee, Business Law Section
State Bar of California
April 12, 2007

Presented by

Konrad L. Trope, Esq.
Novo Law Group, P.C.
4199 Campus Drive, Suite 550
Irvine, California 92612
(949) 509-6531 (tel)
(949) 509-6532 (fax)
ktrope@novolaw.com
www.novolaw.com

Irvine Beverly Hills Washington, D.C.

About the Author:

Konrad Trope is the managing shareholder of the Novo Law Group, P.C., a firm with offices in Irvine, Beverly Hills, and Washington, D.C. Mr. Trope serves an international clientele focusing on Technology, E-Commerce, Telecommunications, and Intellectual Property matters.

He currently serves as the chairman of the VoIP Committee of the American Bar Association—Section of Science and Technology Law. He also serves on the, International VoIP Task Force of the ABA Cyberspace Committee—Business Law Section, investigating regulatory models of VoIP in foreign jurisdictions. In addition, for the past two years, he has served as Chairman of the VoIP/Telecommunications Sub-Committee for the California State Bar Cyberspace Committee.

Mr. Trope has authored more than a dozen articles and presentations concerning Internet security, Internet privacy, government wiretapping, VoIP, and related Internet/e-commerce issues. He is currently writing the *VoIP Handbook*, to be published by the ABA Science & Technology Section.

A 1981 *cum laude* graduate of Pomona College, Mr. Trope attended UCLA School of Law where he was elected as an *Editorial Staff Member* of the **UCLA Law Review.** In addition, while at UCLA Law School, Mr. Trope served as the *Senior Articles Editor* of the **Century City Bar Association Journal,** and the *Associate Editor* of the **Beverly Hills Bar Association Journal.**

Upon graduation in 1985, Mr. Trope moved to Washington, D.C. to serve as law clerk to the Honorable H. Robert Mayer* of the United States Claims Court. Then Mr. Trope went on to serve as law clerk to the Honorable Wilson Cowen, Senior Circuit Judge of the United States Court of Appeals for the Federal Circuit.

In 1987, Mr. Trope joined the Washington, D.C. office of Finley, Kumble, Wagner, Heine, Unterberg, Manley & Casey where he worked in the business, intellectual property and litigation departments. In 1989, he joined the Washington, D.C. office of Foley & Lardner. In 1991, he moved back to Southern California where he founded Novo Law Group.

*Judge Mayer was later elevated to the U.S. Court of Appeals for the Federal Circuit in 1987, and served as Chief Judge of the Federal Circuit from 1993 until 2003.

Privacy and Security Issues in Discovery and Litigation:

Boldly Going Where Disclosure Never Went Before

I. DISCOVERY BY INTERCEPTION OF PRIVATE TELEPHONE CALLS: *Where it all started…..*

In 1928, the U.S. Supreme Court, in a 5-4 decision, legitimized police eavesdropping on telephone conversations. *Olmstead* v. *United States*, 277 U.S. 438, 72 L. Ed. 944, 48 S. Ct. 564 (1928). The interception of this private conversation involved placing metal clips on the telephone wires of Mr. Olmstead. This tapping of the wire or "wiretap" decision commenced an ever expanding debate over issues of privacy and security.

With great trepidation and alarm, Justice Brandeis in his dissent, prophesized that advances in technology would inevitably erode our personal freedoms for privacy and security, liberties guaranteed by the 4th and 5th Amendments:

> "When the Fourth and Fifth Amendments were adopted, "the form that evil had theretofore taken," had been necessarily simple. Force and violence were then the only means known to man by which a Government could directly effect self-incrimination. It could compel the individual to testify -- a compulsion effected, if need be, by torture. It could secure possession of his papers and other articles incident to his private life -- a seizure effected, if need be, by breaking and entry. Protection against such invasion of "the sanctities of a man's home and the privacies of life" was provided in the Fourth and Fifth Amendments by specific language. [citation omitted]. But "time works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.
>
> ….
>
> …The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. …Can it be that the Constitution affords no protection against such invasions of individual security?"

Olmstead v. United States, 277 U.S. at 473-474.

In 1967, as the dawn of the digital age was fulfilling Brandeis' fears that other forms of technological eavesdropping would become possible, the Supreme Court reversed Olmstead. After that, authorities had to get a search warrant before setting wiretaps, even on public payphones.

Congress responded with the passage of the Omnibus Crime Control and Safe Streets Act of 1968, *18 U.S.C. §§ 2501, et. seq., modified and expanded by* Electronic Communications Privacy Act of 1986, *18 U.S.C. §§ 2301, et. seq.* Aside from the search warrant requirement, Congress deliberately authorized the interception of telephonic communications by private parties. So long as "one of the parties to the conversation" consents, then such interception and/or electronic recordation can take place.

In drafting the provision only requiring consent by one party to an electronic communication, Congress sought to provide a remedy against the burgeoning industrial espionage industry. The intent of Congress has not been lost upon the Supreme Court:

> "The legislative history of the 1968 Act indicates that Congress' concern focused on private surveillance "in domestic relations and industrial espionage situations." S. Rep. No. 1097, 90th Cong., 2d Sess., 225 (1968). Similarly, in connection with the enactment of the 1986 amendment, one senator referred to the interest in protecting private communications from "a corporate spy, a police officer without probable cause, or just a plain snoop." 131 Cong. Rec. 24366 (1985) (statement of Sen. Leahy)."

Bartnicki v. Vopper, 532 U.S. 514, 531, n.16 (U.S. 2001)

In stark contrast, states such as Maryland and California require the consent of all parties before a telephone call may be "recorded". Indeed, there have been situation in which Federal and state prosecutors have clashed over the existence of criminal conduct in this area of the law.

Brandeis' warnings against technology assisted discovery and disclosure have largely gone unheeded. Wiretapping by the government or by private parties is explicitly authorized by statute. *See e.g.,* Omnibus Crime Control and Safe Streets Act of 1968, *18 U.S.C. §§ 2501, et. seq., modified and expanded by* Electronic Communications Privacy Act of 1986, *18 U.S.C. §§ 2301, et. seq.*

Over the years, Congress has supposedly been both authorizing the use of evidence obtained by electronic surveillance on specified conditions, and prohibiting its use otherwise. S. Rep. No. 1097, 90th Cong., 2d Sess., 66 (1968). However, the enactment of, *inter alia,:*

1. the Computer Fraud and Abuse Act (*18 U.S.C. §§ 1030)*

2. the Sarbanes-Oxley Act (*18 U.S.C. § 1350*),
3. the Communications Law Enforcement Assistance Act (CALEA) (*47 U.S.C. §§ 1001, et. seq.),* as well as,
4. the Electronic Discovery provisions of the *Federal Rules of Civil Procedure,*

cumulatively provide expanded procedural and substantive tools of compelling disclosure of what otherwise might be considered private information.

Today's Internet and digital technologies support Brandeis' 1928 prediction that "science" would "progress" to where "without removing papers from secret drawers, [litigants] can reproduce them in court, and [thereby] …expose to a jury the most intimate occurrences of the home." *Olmstead,* 277 U.S. at 473-474.

Clients often confront the dilemma between privacy and disclosure, and the security that each provides. These materials will assist the practitioner to:

1. identify some of the more salient issues,
2. suggest some solutions, and
3. still emphasize that that this area of the law is fraught with incessantly developing inconsistencies.

II. The New E-Discovery Rules: An Overview

The 2006 Amendments, effective as of last December 1, only modified *Fed. R. Civ. Proc. 26.* However, Rule 26 establishes the protocols and scheduling by which the parties conduct discovery and/or make mandatory disclosures. Thus, the 2006 Amendments codify and recognize that "documents", "data", and/or "communications" are, in addition to "traditional formats", created, transported and stored in a variety of electronic platforms.

Under the new Rule 26, a party must initially disclose, at the Early Meeting of Counsel, all electronically stored information (ESI), as well as documents that it may use to support its claims or defenses. The term "electronically stored information" has now been defined so that it has the same broad meaning as found in Rule 34(a).

The new amendments also recognize the difficulties in locating, retrieving, and providing discovery of some ESI. Electronic storage systems often make it easier to locate and retrieve information. On the other hand, some sources of electronically stored information can be accessed only with substantial burden and cost.

Therefore, the new amendments establish standards under which the cost and burden of producing ESI is shifted to the requesting party or shared between the parties. Many of the criteria for cost shifting were previously addressed in a series of highly

decisions issued by Judge Shira A. Scheindlin, of the Southern District of New York. *See Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (D.N.Y. 2003).

Plaintiff Laura Zubulake sought various forms of electronic records from her former employer, including deleted e-mails. Judge Scheindlin identified eight factors to be considered in cost shifting a discovery request:

> "(1) the specificity of the discovery requests; (2) the likelihood of discovering critical information; (3) the availability of such information from other sources; (4) the purposes for which the responding party maintains the requested data; (5) the relative benefits to the parties of obtaining the information; (6) the total cost associated with production; (7) the relative ability of each party to control costs and its incentive to do so; and (8) the resources available to each party."

Id. at 316.

The new amendments to Rule 26 not only incorporate these eight factors from the *Zubulake* decision, they also impose specific burdens on the parties. The responding party has the burden as to one aspect of the inquiry--whether the identified sources are not reasonably accessible in light of the burdens and costs required to search for, retrieve, and produce whatever responsive information may be found. On the other hand, the requesting party has the burden of showing that its need for the discovery outweighs the burdens and costs of locating, retrieving, and producing the information.

Ultimately, after the parties "meet and confer" in good faith, the court may have to determine whether the identified sources are not reasonably accessible and whether the requesting party has shown good cause for some or all of the discovery, consistent with the limitations of Rule 26(b)(2)(C), through a single proceeding or presentation.

The good-cause determination, however, may be complicated because the court and parties may know little about what information the sources identified as not reasonably accessible might contain, whether it is relevant, or how valuable it may be to the litigation. Thus, the recent decisions involving the new Rule 26 will be watched very closely. I

As part of the 2006 Amendments, Rule 26 now also requires that the responding party identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing. The identification should, provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources. The duty to preserve ESI is also addressed in these amendments to Rule 26.

III. Impact of the New Rules Upon E-Discovery Disputes and Practices

Attorneys will need to be fully familiar with these new additions to the FRCP in order to discuss E-Discovery protocols at Rule 26(a) meetings and to address E-Discovery issues which will inevitably present themselves throughout the case. Given the rapid, if not exponential, rise in business litigation involving trade secrets, employment disputes, due diligence, and intellectual property, knowledge of the new E-Discovery Rules will be critical.

Courts have been dealing with E-Discovery for several years. Nevertheless, since implementation of the new rules on December 1, 2006, there have been several decisions around the country that dramatically and immediately alter how attorneys need to address E-discovery. Not every case involves the new rules but these cases represent the first wave of decisions that will determine how the ever increasing amount of ESI will be dealt with in the future.

Expect to see numerous, and conflicting, decisions on a variety of E-Discovery issues as courts begin wrestling with interpretation and application of the new rules. This trend will continue throughout 2007 and practitioners should carefully watch for court decisions on key issues including:

1. What are the various forms of “recognized” electronic records?
2. What are the current and developing types of “storage” for electronic records?
3. When is a home computer subject to discovery in business litigation?
4. What production format is acceptable? (.gif, .tif, .pdf)
5. Is native file production required in certain cases?
6. If so, how do you deal with potentially privileged information in those documents, which are not easily redacted or excluded?
7. What kind of record retention policies should a client implement?
8. What kinds of security tools and protocols should a client deploy to protect the security of ESI.

9. Under what circumstances is data considered reasonably accessible and inaccessible?

10. How do courts handle "clawback" provisions for inadvertently disclosed privileged documents?

11. When does such inadvertent such disclosure waive any applicable privilege?

Keep in mind that many states, including California, have already, or are in the process of amending their own rules of civil procedure to mirror the federal amendments regarding ESI. These issues, and many others, will be interpreted and decided by courts everywhere using the new rules as a map.

IV. FORMS OF DATA SUBJECT TO DISCOVERY AND PRIVACY ISSUES

A. Email (including attachments);

B. Word processing documents;

C. Spreadsheets;

D. Presentation documents;

E. Graphics;

F. Animations;

G. Images;

H. Audio, video and audiovisual recordings; and

I. Voicemail.

V. METADATA:

Ancillary electronic information that relates to responsive electronic data, such as information that would indicate whether and when the responsive electronic data was created, edited, sent, received and/or opened. Issues such as:

A. trade secrets;

B. attorney-client privilege;

C. attorney-work product privilege

D. physician-patient privilege

E. husband-wife privilege

are all impacted by whether or not metadata must be disclosed.

VI. DATA TRANSMISSION AND STORAGE

The following forms of data transmission and storage are impacted when addressing issues of privacy and security:

A. Databases;

B. Networks;

C. Computer systems, including legacy systems (hardware and software);

D. Servers;

E. Archives;

F. Back up or disaster recovery systems;

G. Tapes, discs, drives, cartridges and other storage media;

H. Laptops;

I. Personal computers;

J. Internet data;

K. Personal digital assistants;

L. Handheld wireless devices;

M. Mobile telephones;

N. Paging devices; and

O. Audio systems, including voicemail.

P. Voice Over Internet Protocol Systems

Whether potentially producible electronic data may include data that has been deleted but can be restored.

VII. RECENT COURT DECISIONS INTERPRETING THE NEW E-DISCOVERY RULES

Several recent cases address the unique difficulties of dealing with E-Discovery under the new December 1, 2006 Amendments to *Fed. R. Civ Proc. 26.* These new decisions already indicate that the courts will not be unified in their approaches to interpreting the new E-Discovery rules.

Nevertheless, these cases discussed below are instructive for providing guidance to what the courts will likely consider to be the salient problems with E-Discovery.

Ameriwood Industries, Inc., v. Liberman, 2006 WL 3825291 (E.D. Mo. Dec. 27, 2006).

In this trade secrets case, the plaintiff alleged that his former employees, who had formed a competing company, sabotaged plaintiff's business relationships and then diverted those customers to their newly formed company. Plaintiff sought production of "All computer or portable or detachable hard drives, or mirror images thereof, used by [Defendants] since May 2005, including but not limited to any computer or portable or detachable hard drives in their homes."

Plaintiff argued that Defendants forwarded Plaintiff's customer information and other trade secrets from Plaintiff's computers to their personal email accounts. Plaintiff also expressed concern that these documents may have been further disseminated to others and/or deleted to hide the Defendants' actions.

The court sided with Plaintiff and noted that some ESI may not be obtained during a typical search. Citing to the advisory committee notes to Fed.R.Civ.P. 26(f), the court explained: Computer programs may retain draft language, editorial comments, and other deleted matter (sometimes referred to as "embedded data" or "embedded edits") in an electronic file but not make them apparent to the reader. Information describing the

history, tracking or management of an electronic file (sometimes called "metadata") is not usually apparent to the reader viewing a hard copy or screen image.

In granting Plaintiff's discovery request, the court focused upon an email that had been sent from Defendant Liberman's personal email account to one of Plaintiff's customers (Samsung), while Liberman was still employed by Plaintiff. The defendants did not dispute that they had not produced the email in discovery.

In light of the Samsung email, the court found that other emails may exist on defendant's computers as well as other data that could provide answers to Plaintiff's pertinent inquiries regarding the dissemination and whereabouts of his electronic files. Due to the close relationship between Plaintiff's claims and defendants' computer equipment, and having cause to question if defendants had produced all responsive documents, the court allowed an independent expert to obtain and search images of defendants computers.

Flexsys Americas LP, v. Kumho Tire U.S.A., Inc. 2006 WL 3526974 (N.D. Ohio).

In this patent infringement case, Plaintiff searched and produced emails from one individual in response to discovery. Defendant provided evidence that relevant information existed in files for other individuals at the company. Plaintiff objected on the grounds that the complete search requested by the Defendant would be expensive and could not be completed within the necessary time frame.

The court determined that the parties had not reached an agreement on the scope of electronic discovery as contemplated by the amendments to the federal rules. The court recognized the burden for a large corporate entity to search through years of electronic files and balanced that with the fact that Plaintiff had provided significant discovery through earlier production and depositions. The court limited further discovery to 10 individuals chosen by Defendant.

Anadarko Petroleum Corp. v. Davis, 2006 WL 3837518 (S.D. Tex Dec. 28 2006)

In this trade secrets case, Defendant Davis resigned to join GeoSouthern Energy Corporation. Davis admitted that prior to leaving Anadarko, he downloaded confidential and proprietary information from Anadarko's computers. Davis then transferred that information to GeoSouthern's computers. Davis denied any significant use of the information and denied any use to Anadarko's detriment.

On the same day the complaint was filed, Anadarko's counsel sent a litigation hold letter to GeoSouthern. The letter stated:

"Each of you has an obligation to preserve all digital or analog electronic files in electronic format, regardless of whether hard copies of the information exist. This includes preserving:

1. Active data (i.e. data immediately and easily accessible on your systems today);
2. Archived data (i.e. data residing on backup tapes or other storage media); and
3. Deleted data (i.e. data that has been deleted from a computer hard drive but is recoverable through computer forensic techniques).

At the direction of his attorney, Davis began retrieving the Anadarko information he had initially delivered to his own laptop and GeoSouthern's computers. Davis then deleted the Anadarko files from these computers and copied the information he had taken onto a thumb drive to be returned to Anadarko. Davis produced a list of documents he had taken to Anadarko along with the thumb drive.

In addressing Anadarko's request for spoliation sanctions, the court distinguished the case from the typical spoliation scenario. In most cases when a party asserts that spoliation of electronic data has taken place, the party wants the information to remain available in the same form that it was maintained by the other party. Here, Anadarko had specifically requested that all electronically stored confidential and proprietary information taken by Davis be returned and also be made inaccessible to anyone at GeoSouthern. This required that the information be deleted.

Second, in most spoliation cases, when information is deleted, no other record of it exists and it is not promptly produced to the other side as it was here. Third, Davis and GeoSouthern agreed to allow a forensic analysis of their computer systems to ensure that all information taken by Davis was returned and removed.

Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640 (D. Kan. 2005).

This decision has caused much anguish for counsel and clients alike. The Court held that when a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact. Absent a timely objection to production of metadata or stipulation between the parties that the metadata should not be produced, the producing party either produces or should request a protective order.

With many firms using metadata scrubber programs and converting documents to PDF or TIFF files as standard practice, the *Williams* decision continues to be a source of great concern. However, there appears to be an emerging presumption against the production of metadata absent a specific need.

Wyeth v. Impax Labs, 2006 WL 3091331 (D.Del. 2006) .

In denying Impax's request for metadata, the court noted Impax had not shown a particularized need for the metadata and that metadata often provides limited evidentiary value while its review wastes litigation resources.

Kentucky Speedway, LLC v. NASCAR, Inc., 2006 U.S. Dist LEXIS 92028 (E.D. Ky. Dec. 18, 2006).

In denying plaintiff's request for discovery of Defendant's metadata, the Court stated that the holding of Williams v. Sprint requiring production of metadata was "not persuasive" and was not warranted in this case because the Plaintiff made no showing of a particular need for the metadata. In fact, the Court noted that in most cases and for most documents, metadata does not provide relevant information.

VIII. SUGGESTED PRACTICES FOR HANDLING E-DISCOVERY

If you are involved in a case that will involve ESI, you should implement a discovery plan as early as possible.

Traps for the unwary:

1. Blowback everything: Don't think you can just print everything out and review it manually. In large cases involving hundreds of gigabaytes of ESI or more, you will be reviewing millions of pages. Determine what your needs are and discuss these with your E-Discovery vendor who can recommend solutions to streamline review through existing technology and software.

2. Trying to do it themselves: Don't try to figure out page counts, conduct manual reviews, bates number, search by keywords or open encrypted files. Your vendor can do this in a fraction of the time it will take your staff and provide you with a defensible protocol throughout the case.

3. Don't rely on IT. Your IT department is likely not aware of the necessary protocols to ensure authenticity of the data and can unwillingly alter document metadata.

4. Trying to be an expert: Don't assume you are the best person to strategize a massive ESI production. Attorneys need to focus on important discovery issues, spoliation, relevancy, case strategy and file preservation. Using your IT

staff in conjunction with an outside vendor will help you prepare the case better, faster and cheaper.

IX. ANTI-SPOLIATION PROTOCOLS

As concerns over privacy increase in litigation, so too does the problem with spoliation of evidence, both intentional and inadvertent. The sample letter below presents the scope and breadth of anti-spoliation risks that should be addressed in the early stages of any litigation action.

Firm Letterhead

Counsel for Defendant
Address
City, State, Zip

Re: Preservation of Electronic and Documentary Evidence

Dear

This letter is a preservation of evidence request to each and every Defendant, or his/her/its counsel, if said counsel have formally appeared, in the above referenced matter, along with their heirs, agents, assigns, attorneys, accountants, partners, officers, directors, employees and agents[1] (both past, current and future.). Further, if any officers, directors, employees, agents or independent contractors involved in this matter from August, 2003 to the present, are no longer in your employ, we ask for you to also preserve the data described in this letter that was in their care, custody and control in the same manner as those currently employed.[2]

Please note, that under FRCP 26(a) (1) (B) we expect disclosure of the data and documents described in this letter as part of your initial discovery disclosures, for the period January 1,2004 to the present. Litigants owe an "uncompromising duty to preserve" what they know or reasonably should know will be relevant evidence in a pending lawsuit. *Kronisch v. United States,* 150 F.3d 112, 130 (2nd Cir. 1998); *Sensonics, Inc. v. Aerosonic Corp.,* 81 F.3d 1566, 1575 (Fed.Cir. 1996), *Mathias v. Jacobs,* 197 FRD 29, 37 (Fed.Cir. 1996).

---

[1] As referred to herein, the term "Defendant" means not only the current Defendant, but also those persons, organizations or corporations that act in concert or in participation with it, or acting or purporting to act on its behalf over whom Defendant have control, access or direction.

[2] If an employee has terminated their employment who had a computer or who had access to a computer, this request is for you to also preserve all electronic data from their particular computer, including electronic mail, databases, word processing files and the like. We will be asking for production of information in the future for you to identify such computers, electronic databases, files and the like, and are hereby requesting that such information be retained in its existing state, for this litigation. Any destruction or overriding or erasure of electronic data will be considered spoliation. *Jacobs,* 197 FRD 29, 37 (Fed.Cir. 1996).

The duty to preserve exists where a party "is on notice that documents and information in its possession are relevant to litigation . . . or are reasonably calculated to lead to the discovery of admissible evidence." *Bayoil, S.A. v. Polembros Shipping Ltd.,* 196 FRD 479, 482, (S.D. Tex. 2000); *Wm. T. Thompson Co. v General Nutrition Corp., Inc.,* 593 F.Supp. 1443, 1455, (C.D. Cal. 1984).

"The obligation to retain discoverable materials is an affirmative one; it requires that the agency or corporate officers having notice of discovery obligations communicate those obligations to employees in possession of discoverable materials." *National Ass'n. Of Radiation Survivors v. Turnage,* 115 F.R.D. 543, 557058 (N.D. Cal. 1987); *see also Wiliam T. Thompson Co. v. General Nutition Corp.,* 593 F.Supp. 1443, 1455 (C.D. Cal. 1984) (party has duty to preserve what it knows or reasonably should know to be relevant evidence.)

Specifically, Plaintiff requests that each and every Defendant preserve the following:

(I) All electronic mail, including deleted mail and remnants of deleted mail, and information about electronic mail (including message contents, header information and logs of electronic mail system usage.) This includes any:

(a) sent to any DEFENDANT'S employees, customers, prospective customers, members, existing or potential vendors/suppliers with whom any employees, officers, or directors were in contact with or from whom any employees, officers, or directors have as potential/prospective sources of business while employed by Defendant;

(b) received from any DEFENDANT'S employees, customers, prospective customers, members, existing or potential vendors/suppliers identified/defined/specified as participating in the April 28 - May 2, 2004 boat show;

(c) that relates in any way to any duties and obligations by any employees, customers, prospective customers, existing or potential vendors/suppliers, and/or any former employee, contractor and/or consultant to DEFENDANT; and

(d) sent by any employees, officers and/or directors to him/herself or to each other while that employee, contractor and/or consultant was still employed by DEFENDANT and that relates, refers or pertains to the formation, establishment, plans or business of Defendant, along with any that states any person's resignation from Defendant's employ.

(II) All databases (including all records and fields and structural information in such databases) containing information:

(a) referring to DEFENDANT'S employees, customers, prospective customers, members, existing or potential vendors/suppliers identified/defined/specified/referred to above in I. (a) and (b);

(b) initially drafted, created, and/or established by any individual(s) and/or entity while employed or having a relationship with DEFENDANT;

(c) about DEFENDANT'S employees, customers, prospective customers, members, existing or potential vendors/suppliers identified/defined/specified/referred to above in I. (a) and (b);

(d) that relates in any way to DEFENDANT'S employees, customers, prospective customers, existing or potential members, and/or vendors/suppliers duties and responsibilities as an employee, contractor, customer, member and/or consultant to Defendant;

(III) All logs of activity on computer systems that may have been used to process or store electronic data containing information:

(a) referring to DEFENDANT'S employees, customers, prospective customers, members, existing or potential and/or vendors/suppliers identified/defined/specified/referred to above in I. (a) and (b);

(b) initially drafted, created, and/or established by any individual(s) and/or entity while employed or having a relationship with DEFENDANT;

(c) about DEFENDANT'S employees, customers, prospective customers, members, existing or potential vendors/suppliers identified/defined/specified/referred to above in I. (a) and (b); and

(d) that relates in any way to DEFENDANT'S employees, customers, prospective customers, existing or potential members, and/or vendors/suppliers duties and responsibilities as an employee, contractor, customer, member and/or consultant to Defendant;

(IV) All word processing files and file fragments, including deleted and remnant data containing information:

(a) referring to DEFENDANT'S employees, customers, prospective customers, members, existing or potential vendors/suppliers identified/defined/specified/referred to above in I. (a) and (b);

(b) initially drafted, created, and/or established by any individual(s) and/or entity while employed or having a relationship with DEFENDANT;

(c) about DEFENDANT'S employees, customers, prospective customers, members, existing or potential vendors/suppliers identified/defined/specified/referred to above in I. (a) and (b); and

(d) that relates in any way to DEFENDANT'S employees, customers, prospective customers, existing or potential members, and/or vendors/suppliers duties and responsibilities as an employee, contractor, customer, member and/or consultant to Defendant;

(V) All electronic data and file fragments created by application programs which process financial, accounting and billing containing information

(a) referring to DEFENDANT'S employees, customers, prospective customers, members, existing or potential vendors/suppliers identified/defined/specified/referred to above in I. (a) and (b);

(b) initially drafted, created, and/or established by any individual(s) and/or entity while employed or having a relationship with DEFENDANT;

(c) about DEFENDANT'S employees, customers, prospective customers, members, existing or potential vendors/suppliers identified/defined/specified/referred to above in I. (a) and (b); and

(d) that relates in any way to DEFENDANT'S employees, customers, prospective customers, existing or potential members, and/or vendors/suppliers duties and responsibilities as an employee, contractor, customer, member and/or consultant to Defendant;

(VI) All electronic data files and file fragments where such data files contain information found on, or created on, or transferred to (1) desktop computers or workstations; (2) all servers related to Defendant's businesses; (3) any and all laptop computers used or owned by Defendant; (4) hand-held computers used or owned by Defendant, (5) Palm pilot type computers used or owned by Defendant, (6) cell-phone and PSTN voice messaging systems), and (7) third party repositories, where such data files contain information:

(a) referring to DEFENDANT'S employees, customers, prospective customers, members, existing or potential vendors/suppliers identified/defined/specified/referred to above in I. (a) and (b);initially drafted, created, and/or established by any individual(s) and/or entity while employed or having a relationship with DEFENDANT;

(b) about DEFENDANT'S employees, customers, prospective customers, members, existing or potential vendors/suppliers identified/defined/specified/referred to above in I. (a) and (b); and

(c) that relates in any way to DEFENDANT'S employees, customers, prospective customers, existing or potential members, and/or vendors/suppliers duties and responsibilities as an employee, contractor, customer, member and/or consultant to Defendant;

(VII) All other electronic data containing information

(a) referring to DEFENDANT'S employees, customers, prospective customers, members, existing or potential vendors/suppliers identified/defined/specified/referred to above in I. (a) and (b); and

(b) initially drafted, created, and/or established by any individual(s) and/or entity while employed or having a relationship with DEFENDANT;

(c) about DEFENDANT'S employees, customers, prospective customers, members, existing or potential and/or vendors/suppliers identified/defined/specified/referred to above in I. (a) and (b); and

(d) that relates in any way to DEFENDANT'S employees, customers, prospective customers, existing or potential members, and/or vendors/suppliers duties and responsibilities as an employee, contractor, customer, member and/or consultant to Defendant;

(VIII) All paper documents containing information:

(a) referring to DEFENDANT'S employees, customers, prospective customers, members, existing or potential vendors/suppliers identified/defined/specified/referred to above in I. (a) and (b);

(b) initially drafted, created, and/or established by any individual(s) and/or entity while employed or having a relationship with DEFENDANT;

(c) about DEFENDANT'S employees, customers, prospective customers, members, existing or potential vendors/suppliers identified/defined/specified/referred to above in I. (a) and (b); and

(d) that relates in any way to DEFENDANT'S employees, customers, prospective customers, existing or potential members, and/or vendors/suppliers duties and responsibilities as an employee, contractor, customer, member and/or consultant to Defendant;

To minimize the risk of spoliation of relevant electronic and paper documents, each and every Defendant should also observe the following:

A. Do not modify or delete any electronic data files that are maintained in on-line storage and/or direct access storage devices which exist as of the delivery of this letter, pertain to electronic equipment and meet the criteria of paragraphs I-VIII unless a true and correct copy of each such electronic data file has been made; a Directory print is made of those electronic data files, and steps have been taken to ensure that such copy will be preserved and accessible to Plaintiff or anyone acting on its behalf;

B. Cease and desist from any activity that may result in a loss of electronic data pertaining to any electronic equipment and in electronic media used for off-line storage, including magnetic tapes, cartridges and other media. This activity includes (but is not limited to) the suspension of activities involving the rotation, destruction, overriding and/or erasure of such media in while or in part;

C. Preserve any electronic data storage devises and/or media that may contain electronic data pertaining to electronic equipment which may be replaced due to failure and/or upgrade for any reason;

D. Do not alter or erase electronic data pertaining to electronic equipment and do not perform any other procedures (such as data compression and disk de-fragmentation or optimization routines) that may impact such data on any stand-alone micro computer and/or network workstations, unless a true and correct copy has been made of such active files and of completely restored versions of such deleted electronic files and file fragments and unless copies have been made of all directory listings

(including hidden files) for all directories and sub-directories containing such files, and unless arrangements have been made to preserve copies;

E. Preserve copies of all application programs and utilities that may be used to process electronic data pertain to the electronic equipment;

F. Maintain an activity log that documents all modifications made to any electronic data processing system that may affect the systems capability to process any electronic data pertaining to the electronic equipment; and

G. Immediately suspend any and all policies and/or procedures regarding the destruction of documents.

Plaintiff also requests that each and every Defendant take the following steps immediately with respect to *all personal computers* used by Defendant, their heirs, assigns, attorneys, accountants, agents, partners, officers, directors, employees, and independent contractors over which they have control. This includes the officers, directors, employees, agent's, and independent contractors' personal computers outside of Defendant's immediate ownership, but used by such officers, directors, employees, agents, independent contractors, occasionally in their business as an officer, director, employee, agent, or independent contractor of Defendant.

A. Either remove such personal computers from service to preserve the integrity of deleted data or create and maintain forensic image (physical) backups of all data on the drives.

B. Create and maintain full directory listings (including hidden files) for all directories and sub-directories (including hidden directories) on such fixed drives.

C. Collect and store all floppy diskettes, magnetic tapes and cartridges, and other media in connection with such computers prior to the date of delivery of this letter containing any electronic information relating in any manner to the matters in dispute.

D. Take whatever steps are appropriate to preserve relevant evidence created subsequent to this letter.

The preservation procedures set forth above should be observed by each and every Defendant regardless of their individual or personal opinions as to the merits of the

claims and/or as to whether the information subject to preservation will be discoverable. Also, the preservation procedures set forth above should continue and copies of all electronic information and paper documents referred to herein should be retained until the final conclusion of this matter.

Please contact us if you have any questions or comments regarding any of the foregoing or if you and/or your firm no longer represents any of the above-named individuals and/or entities.

Very Truly Yours,

Plaintiff's Counsel

X. EXPEDITED DISCOVERY: ANOTHER ANTI-SPOLIATION TECHNIQUE

Plaintiffs often face the "Catch-22" dilemma having the burden of proof, while the Defendants frequently hold most of the incriminating evidence. This is the conundrum faced by most plaintiffs in intellectual property infringement, employment discrimination, and trade secret misappropriation cases. The expansion of computer and Internet technologies has exacerbated this "discovery dilemma". Digital and Internet technologies, deployed by the defendant, will frequently facilitate both the commission of the tort and the subsequent destruction of the very evidence necessary for proving Plaintiff's claims for relief.

Moreover, discovery in federal cases is typically "on hold" until after the court conducts its Scheduling Conference under *Fed. R. Civ. Proc. 16.* Consequently, the stay on discovery can last anywhere from a month to three months. *See Id.*

Courts are showing increased willingness to consider applications for expedited discovery, thus circumventing, at least partially, the initial hold on discovery procedures. *See, e.g.,:*

Ameriwood Insturstires, Inc. v. Liberman, 2006 WL 3825291 (E.D. Mo. Dec. 27, 2006) (court granted Plaintiffs request for expedited discovery under the newly enacted Federal Electronic Discovery Rules including ordering Defendants to facilitate access to their hard drives and to reveal "meta-data", as well as ordering Defendants to immediately cease any activity that would alter or modify the contents of their "hard drives");

UMG Recordings v. DOES 1-4, 2006 U.S. Dist. LEXIS 32821 (N.D. Cal. March 6, 2006) (plaintiff's application for expedited discovery granted for good cause: little if any prejudice to Defendants, great risk of destruction of computer data, copyright claims involve risk of irreparable harm);

Physicians Interactive v. Lathian Systems, Inc., 2003 U.S. Dist. LEXIS 22868 (E.D. Va., 2003) (court grants expedited discovery request to plaintiff website suing defendants under CFAA where Plaintiff demonstrated good cause in that there was high risk of destruction of the evidence sought and the resulting irreparable harm to plaintiff).

XI. PROTECTION OF ELECTRONICLY STORED TRADE SECRETS

In today's business litigation landscape, these cases often involve allegations concerning the use of computers, email and other technology. As technology advances, it gets easier everyday for individuals to steal data and intellectual property through use of memory sticks, flash drives and even I-Pods ("pod slurping").

These devices can hold up to 40+ gigabytes of data. Consequently, depending on the type of document, a gigabyte might contain up to several hundred thousand pages of information). With the size of such devices shrinking on almost a monthly basis, employers face a grim reality that an employee could walk out the door with the company's entire intellectual property and trade secret portfolio in his pocket.

This kind of activity is specifically addressed in the Computer Fraud and Abuse Act, *18 U.S.C.S. § 1030.* A defendant triggers liability, *inter alia*, by knowingly accessing a protected computer system without authorization and as a result obtained "anything of value". *18 U.S.C.S. § 1030(a) (4).*

Moreover, the quantum of proof necessary to demonstrate misappropriation of trade secrets (and tortious interference with economic relations) is relatively low when "the secret itself is so unique that any form of duplication would probably be improper."

Pioneer Hi-Bred Int'l. v Holden Found. Seeds, 35 F.3d 1226, 1240 (8th Cir. 1994) *citing with approval Rockwell Graphic Sys., Inc. v. DEV Ind., Inc.*, 925 F.2d 174, 178 (7th Cir. 1991).

Indeed, the greater the level of security instituted by the Plaintiff to protect its Trade Secrets, the less quantum of proof necessary for demonstrating misappropriation of trade secrets and tortuous interference. *See Pioneer*, at 1240 *citing Anaconda Co. v Metric Tool & Die Co.*, 485 F.Supp. 410, 421-22 (E.D. Pa. 1980).

In short, if "the [trade] secret itself is so unique that any form of duplication would probably be improper," then the trier of fact [may] assume that the defendant is the *likely source of the illegal disclosure. See Pioneer*, at 1240 and *Brown*, at 825.

CONCLUSION

What does the future of privacy and E-Discovery look like? Not that long ago, we couldn't have conceived of everyday gadgets like I-pods or cell phones that play songs, take pictures and have navigation systems. As technology continues to evolve, the form and amount of ESI will continue to grow as well. Attorneys will need to continually educate themselves on emerging technologies and be flexible in allowing for new and unforeseen issues.